APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/797,920	03/09/2004	Kenneth L. Levy	P0951	3347

23735   7590   02/24/2010
DIGIMARC CORPORATION
9405 SW GEMINI DRIVE
BEAVERTON, OR 97008

EXAMINER
CORBO, NICHOLAS T

ART UNIT	PAPER NUMBER
2427	

MAIL DATE	DELIVERY MODE
02/24/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Application Number: 10/797,920
Filing Date: March 09, 2004
Appellant(s): LEVY, KENNETH L.

William Y. Conwell
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 10/21/2009 appealing from the Office action

mailed 04/21/2009.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows:

WITHDRAWN REJECTIONS

The following grounds of rejection are not presented for review on appeal because they have been withdrawn by the examiner. The rejection of claims 11, 14, and 15 under 35 U.S.C. 101.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

20030217122	Roese et al	11-2003
20010044899	Levy	11-2001
20020186844	Levy et al	12-2002
20050071663	Medvinsky et al	03-2005

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21 (2) of such treaty in the English language.

2. Claims 4, 7-9, 11, and 13-17 are rejected under 35 U.S.C. 102(e) as being anticipated by Roese et al. (US 2003/0217122 A1 hereinafter Roese).

Regarding claim 4, Roese discloses "a method of providing entertainment content from a distributor to a home, while governing potential redistribution of the content from the

home, the method including forming an IP packet having header data and body data,

wherein the body data includes content data, and the header data includes a first

destination address within the home to which the distributor intends the content data be

delivered, the method comprising:

the distributor forming said header data to additionally include additional data specifying

whether it is permissible to send a copy of the content data in the packet to a second

destination address different than the first destination address, wherein the additional

data has at least two states, respectively indicating: ([0115]-[0117], a tag is used for

generating a packet with additional data for placing transmission restrictions as

described above)

(a) it is not permissible to send a copy of the content data in the packet to any second

destination address; or" ([0115], Fig. 1, where paragraph [0115] of Roese states

'defined boundaries (e.g., a present device, a room, ...' where the tag incorporates both

states being that the tag may prohibit transmissions to certain destinations or prohibit

transmissions to any destination that is outside present device meaning transmissions

to any location from the present device is prohibited)

"(b) it is not permissible to send a copy of the content data in the packet to any second

destination address except to a second destination address within a domain that also

includes the first destination address" ([0115]-[0118], Fig. 6, describes preventing the

data from being sent to any other destination, [0117] describes selectively preventing

data from being sent to any destination outside of a set domain, [0115] describes a

device may not transmit data to any other destination outside a domain, where no

device may be authorized to receive the content no matter the device location).

"wherein said domain comprises networked devices associated with a single family, and

restriction on the potential redistribution of the content is defined by reference to the

intended first address" ([0115], any devices that belong to a single entity such as a

campus regardless of who uses the devices belonging to the single entity constitutes as

a domain of network devices associated with a single family where the restrictions on

the exchanging the content may be limited to within the domain of the single family such

as any network devices within a campus)

Regarding claim 7, Roese discloses "the method of claim 4 wherein a device associated

with the first destination address has a first physical location and a device associated

with the second destination address has a second physical location, and the additional

data includes a field signaling that copying of data in said packet to said second

destination address should be:

(a) permitted if the second physical location is physically proximate to the first physical

location; and

(b) prohibited if the second physical location is physically remote from the first physical

location" ([0100]-[0103] describes the location limitation being a physical location

limitation)

Regarding claim 8, Roese discloses "the method of claim 7 wherein the first and second

destination addresses are within a common domain" ([0100]-[0103], Fig. 1, Fig. 8,

where the first and second destination devices can be within a common domain).

Regarding claim 9, Roese discloses "the method of claim 7 wherein the first and second

destination addresses both correspond to network devices associated with a single family" ([0100]-[0103], Fig. 1, Fig. 8, network devices allowed within the network may be limited to a single family).

Regarding claim 11, Roese discloses "a method of data processing that includes receiving an IP packet having header data and body data, wherein the header data includes a first destination address, the first destination address corresponding to a device at a first physical location where delivery of the packet was intended by an originator thereof, the body data comprising content data, the method comprising - at said first physical location - interpreting additional data in the header of said packet as specifying whether it is permissible to re-transmit a copy of data in the packet - after receipt thereof at the first destination address - to a second destination address, wherein:" (Roese teaches both generating an IP packet with additional data conveying restriction information at a first device location, Fig. 1 item 104, as described in claim 4 above, and receiving and analyzing the generated IP packet at a second device location, Fig. 1 item 114, such as a firewall as described in the response to arguments above. Where at the second device it is determined as stated in paragraph 117 "if the data is going to be routed in the next hop to a location that is outside the permitted location(s)" thus the destination of the packet determined in the packet header is analyzed for determining hops and enforcing restrictions on the packet)

"(a) if the additional data has a first state, prohibiting re-transmission of a copy of the content data in the packet to any second destination address; and" ([0115]-[0117], the packet received at the second device determines according to the additional data that

the packet is in a first state being that it is prohibited from any transmission outside the

first device and the second device accordingly prohibits further transmission)

"(b) if the additional data has a second state, prohibiting re-transmission of a copy of

data in the packet to any second destination address other than a second destination

address within a domain that also includes the first destination address"

([0115]-[0117], when the second device receives the packet and determines according

to the additional data that the packet is in a second state being that transmission is

allowed but also prohibited from transmission to devices not within a set region, the

second device will accordingly prohibit further transmission when it is determined the

next hop for the packet to be routed to is not a physical location within a specified

region, where the destination of the packet determined in the packet header is a

determining factor in the hops).

Regarding claim 13, the claim is rejected for the same reasons as claim 4

above.

Regarding claim 14-16, the claim is rejected for the same reasons as claims 7-9 above,

respectively.

Regarding claim 17, Roese discloses "the method of claim 14 wherein the method

includes determining whether the second physical location is physically remote from the

first physically location by reference to whether the second destination address is

served by a common firewall with the first destination address ([0098] describes

combining the use of a firewall with the physical locations of the devices, where it states

a firewall makes determination of packets into and out of a network).

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 10, 18, 25-26, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roese et al. (US 2003/0217122 A1 hereinafter Roese) in view of Levy (US 2001/0044899 hereinafter '899).

Regarding claim 1, Roese discloses "a method of enforcing geographical restrictions on content redistribution in a TCP/IP network in which content is distributed in packet form, each packet including header data and content data, the header data comprising information about the packet and its payload, the method comprising the acts: defining a geographical boundary across which certain content data does not pass, wherein said boundary is defined--at least in part--by a hardware firewall device" ([0098], [0115]-[0118], Fig. 6, where [0098] describes the use of firewalls with devices sending and receiving content information, [0117] describes preventing the data from being transmitted at the point of transmission or at the point of reception depending on assigned restrictions of the data).

"determining whether an IP packet should be regarded as conveying content that should

not cross said boundary," by reference to one or more single-bit flags included in the

header data of said packet" ([0115]-[0118], Fig. 6, where step 620 in Fig. 6 is where

data being transmitted is tagged with information about a boundary restriction, and

[0116] describes the tagged information being conveyed in the data packets being

transmitted such that a device receiving the packet may appropriately restrict the packet

upon analyzing).

But, while Roese states that a system determines the location sensitivity of data to be

transferred and placing additional data in a generated packet to identify restriction

information at receiving devices ([0116]), Roese does not explicitly state placing the

additional data as a packet header containing flag bits being "related to the payload of a

watermark in the content". However, '899 discloses transmarking video entertainment

data to preserve the use of a video entertainment data digital "watermark in the content"

when modifying the signal of the video entertainment data including packetizing the

video entertainment data ([0012]-[0013], [0015], [0019]).

'899 teaches that a watermark is first detected ([0022]) in an original embodiment of the

data and information such as copy control parameters and content identifiers are

extracted ([0023]). Subsequently, the detected watermark signal may or may not be

removed ([0026]), and a second watermark is then added based on the first detected

watermark ([0029]) where the second watermark is adapted to work in the intended

environment ([0033]) such as a packet-based communication channel, where a packet

header with information pertaining to a watermark payload in each packet is generated

([0035]).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time
the invention was made to combine the teachings of '899 for preserving
watermarks of digital content during transmission in a packet-based communication
channel via transmarking an initial digital watermark of the content into watermark
payloads in each packet with additional data placed in each packet header based on the
watermark payload with the teachings of Roese for modifying packets with additional
data based on tags, such that the additional data may convey restriction information on
the data in the packets for devices to determine whether to prohibit or allow
transmission of packets. One would have been motivated to do so to provide restriction
on content as intended free from malicious user intervention by referring to a payload of
a watermark in the body data to determine the usage rules in a packet header, where
Roese seeks to provide secure restriction on usage of content and a watermark
securely provides restriction information hidden from a user.

Regarding claims 10 and 18, Roese teaches the method of claim 4 and 11 as described
above, but Roese does not explicitly state "wherein said additional data is related to the
payload of a watermark encoded in the body data". However, placing header
information containing flag bits related to a watermark has been analyzed as in claim 1
above.

Regarding claims 25-26 and 28, Roese teaches the use of a tag for defining boundaries
as described in paragraph 115, where paragraph 116 states "the server generating a
data packet to transport the data over the network can add this tag while generating the
data and/or packet", Roese states in paragraph 117 "a device within system 100 and/or

the data itself determines (step 625) whether the data is outside the permitted

location(s)" and paragraph 98 teaches the device limiting the packet transmission in

system 100 of Fig. 1 being a firewall, where paragraph 98 states "firewalls are primarily

computer programs designed to analyze packets and, from that analysis, make a

determination as to whether packet transmission into or out of the network is permitted".

Therefore, data added to the packet based on the tag during generation of the packet

includes the given additional data, where the firewall may analyze the body or header of

the packet received, it is understood that both placing additional data in the header

and/or the packet is taught such that the firewall has means to properly analyze the

additional data of the packet to determine restrictions.

But, Roese does not explicitly state "extracting restriction information from header data

conveyed with the video entertainment" or "discerning the restriction information by

reference to data decoded from digital watermark information hidden within the video

entertainment" and "including data indicating said ascertained restriction information in

header portions of each of said IP packets".

However, '899 discloses transmarking video entertainment data to be preserve the use

of a video entertainment data digital watermark when modifying the signal of the video

entertainment data including packetizing the video entertainment data ([0012]- [0013],

[0015],[0019]). '899 teaches that a watermark is first detected ([0022]) in an original

embodiment of the data and information such as copy control parameters and content

identifiers are extracted ([0023]). Subsequently, the detected watermark signal may or

may not be removed ([0026]), and a second watermark is then added based on the first

detected watermark ([0029]) where the second watermark is adapted to work in the
intended environment ([0033]) such as a packet-based communication channel, where
a packet header with information pertaining to a watermark payload in each packet is
generated ([0035]). Additionally, '899 discloses converting a header of the video
entertainment data into a watermark ([0016]) such that a watermark payload and packet
header pertain to the header of the video entertainment data.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time
the invention was made to combine the teachings of '899 for preserving watermark and
header information of a video entertainment data by placing information pertaining to
the watermark and header data into the packet header with the teachings of Roese for
placing tag information into the header of the packet based on the data packetized to
enforce geographical limitations on exchanging the data. One would have been
motivated to do so to provide restriction on content as intended free from malicious user
intervention by referring to a watermark in the data to determine the usage rules, where
Roese seeks to provide secure restriction on usage of content and a watermark
securely provides restriction information hidden from a user.

5. Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over Roese et al.
(US 2003/0217122 A1 hereinafter Roese) in view of Levy (US 2001/0044899
hereinafter '899) and in further view of Levy et al. (US 2002/0186844 hereinafter '844).
Regarding claim 27, Roese and '899 teach claim 25 as disclosed above, but do not
explicitly teach obtaining restriction information from a remote repository. However,
'844 states the use of obtaining a content identifier from a video entertainment data

digital watermark using the content identifier to retrieve usage restrictions imposed on the video entertainment data from an external database ([0025]-[0026], Fig. 1).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teachings of '844 for obtaining restriction information from a remote repository associated with the video entertainment data via a content identifier determined by the digital watermark with the teachings of Roese and '844 where restriction information based on data to be transmitted imposing geographical limitations is placed in the header of a packet. One would have been motivated to do so to further improved the teachings of '844 for using a digital watermark embedded in video entertainment data whereby accessing restriction information pertaining to the digital watermark that may not have been entirely contained within the digital watermark so as to provide a option of updating of the restriction information a remote database.

6. Claim 29 is rejected under 35 U.S.C. 103(a) as being unpatentable over Roese et al. (US 2003/0217122 A1 hereinafter Roese) in view of Levy (US 2001/0044899 hereinafter '899), and in further view of Medvinsky et al. (US 2005/0071663 hereinafter Medvinsky).

Regarding claim 29, Roese and '899 teach the methods of claim 1 as described above, but do not explicitly state the use of a single bit flag. However, Medvinsky teaches the use of a Boolean flags which to represent DRM functions including a Boolean flag representing whether it may be moved to another location that is an authorized domain ([0168]).

Therefore, it would have been obvious to combine the teachings of Roese and '899 for use of header data to enforce geographical restrictions on transmission of data with the teachings of Medvinsky for use of single-bit Boolean flags representing whether data may be transmitted to another location that is an authorized domain. One would have been motivated to use a single-bit flag in the header data to reduce data sizes of packets and lower computational power necessary to process the additional header data pertaining to geographical restriction.

7. Claims 30-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roese et al. (US 2003/0217122 A1 hereinafter Roese) as applied to claims 4 and 11, and in view of Medvinsky et al. (US 2005/0071663 hereinafter Medvinsky).

Regarding claims 30-31, Roese teaches the methods of claims 4 and 11 as described above, but do not explicitly state the use of a single bit flag. However, Medvinsky teaches the use of a Boolean flags which to represent DRM functions including a Boolean flag representing whether it may be moved to another location that is an authorized domain ([0168]).

Therefore, it would have been obvious to combine the teachings of Roese for use of header data to enforce geographical restrictions on transmission of data with the teachings of Medvinsky for use of single-bit Boolean flags representing whether data may be transmitted to another location that is an authorized domain. One would have been motivated to use a single-bit flag in the header data to reduce data sizes of packets and lower computational power necessary to process the additional header data pertaining to geographical restriction.

(10) Response to Argument

In response to appellant's arguments, the Examiner respectfully disagrees that the rejection should be reversed. Only those arguments raised by the appellant pursuant to the particular issues on appeal have been considered and addressed by the Examiner. Any further arguments regarding particular limitations not specifically argued or other reasoning regarding deficiencies in a prima facie case of obviousness that the appellant could have made are considered as having been conceded by the appellant for the bases of the decision of this appeal and are not being subsequently addressed by the Examiner for the Board's consideration. Should the panel find that the Examiner's position/arguments or any aspect of the rejection is not sufficiently clear or a particular issue is of need of further explanation, it is respectfully requested that the case be remanded to the Examiner for further explanation prior to the rendering of a decision.[1]

1. Rejection of claims 11, 14, and 15 under 35 U.S.C. 101

As stated above, this rejection was withdrawn by the Examiner as noted in the Advisory Action mailed on 07/31/2009, and thus will not be presented for review on appeal.

2. Rejection of claim 4 under 35 U.S.C. 102 using Roese

---

[1] See 37 CFR 41.50(a)(1) and MPEP 1211

A. Regarding Appellant's argument alleging that the tag of Roese "has only one single state" (Page 10, Para 5), the Examiner respectfully disagrees. While the example provided by the Appellant only discloses one example of a state for the tag (interpreted to be the "additional data") to possess, Paragraph 0115 of Roese clearly teaches multiple states (e.g., device, room, building, campus, city, country). While Appellant is trying to imply that the tags/additional data of Roese do not possess these various states, the Examiner defends the position taken in the Office Action dated 04/21/2009. As seen in Appellant's Appeal Brief, Appellant discloses that "'additional data' has **one of two states**" (emphasis added). The position taken by the Examiner in the Office Action dated 04/21/2009 discloses the first state in the event that the defined boundary defined by the tag/additional information is a present device/first destination device, wherein the information received will not be permitted to be transmitted beyond that device, thereby meeting the limitations of state "(a)" seen in claim 4. The same teaching applied to one of the other states presented in Paragraph 0115 (room, building, campus, city, country) meets the limitations of state "(b)" seen in claim 4 due to the fact that each successive state is an example of a larger domain encompassing that current device/first destination address that the transmission of the information will be limited to occur within. As stated by Appellant, these two states merely need to be possessed by the additional data/tags and need not occur simultaneously.

B. Regarding Appellant's argument alleging the Examiner's "interpretation of the claim that somehow makes the user in the home also the claimed 'distributor' is too tortured to be sustained" (Page 11, Para 2), the Examiner respectfully disagrees. In

giving the claims their broadest reasonable interpretation, the role of the distributor is not defined by the claim language to occur at a location that is necessarily separate from the home. No supported reasoning is provided by the Appellant as to why the user at the home is entirely incapable of forming packet header data with the additional data. Nothing in the art would be understood by a person having ordinary skill in the art that would prevent a user in conjunction with the use of a computer at the home from creating packet headers from typical interactions with the Internet.

C. Regarding Appellant's argument alleging "Roese does not test any relation between an original address and a subsequent address in deciding whether re-distribution is permitted" (Page 11, Para 6), the Examiner respectfully disagrees. As disclosed above in section 10-2A, Roese discloses the relation between the original address (the present device) and a subsequent address (any address within any of the domains containing the present device, e.g. the room, building, campus, city, country the current device is in) in deciding whether redistribution is permitted within or beyond each of those boundaries (depending on if any of those boundaries are set) (Para. 15).

D. Regarding Appellant's argument alleging Roese does not disclose "networked devices 'associated with a single family'" (Page 12, Para 3), the Examiner respectfully disagrees. The Examiner pointed to an example of one of the states listed in Paragraph 0115 of Roese (campus) to address this claim limitation. The Appellant does not disclose any supported reasoning as to why the Examiner's interpretation does not meet the claim limitation. Neither does Appellant's specification define "family" to have any meaning other than a common definition, such as "any group of related things" as

defined by Collins English Dictionary. The "family", as interpreted in the example stated
in the Office Action dated 04/21/2009 by the Examiner, is all devices that is networked
within the campus boundaries.

E. Regarding Appellant's argument alleging "the restriction in Roese is not
defined by reference to the intended first address" (Page 12, Para 4), the Examiner
respectfully disagrees. As stated above in sections 10-2A and 10-2C, Roese discloses
the restrictions that are placed on the information by the additional data/tag stem from
going *beyond* a present/current device, the relationships branching outward form the
device to the room, building, campus, city, country that houses the present device (Para
0115).

3. Rejection of claim 7 under 35 U.S.C. 102 using Roese

Regarding Appellant's argument alleging the paragraphs cited by the Examiner in
the Office Action dated 04/21/2009 "do not concern re-distribution of entertainment
content from an intended destination address to a second address" (Page 13, Para 2),
the Examiner respectfully disagrees. While a small portion of the cited paragraphs of
Roese does explain that logins are an expanded feature of the authentication/location
server's location database, these Paragraphs are more detailed explanations as to
features explained in Paragraphs 0096-0099, wherein the location of a user requesting
data (from a 2nd location) is compared to that of where the data is presently location (a
1st location). Therefore, the rejection presented by the Examiner is not directed at any
concept that is unrelated, as alleged by the Appellant.

4. Rejection of claim 8 under 35 U.S.C. 102 using Roese

Regarding Appellant's argument alleging the figures cited by the Examiner (Figs. 1 and 8) "have no teachings about a common domain", the Examiner respectfully disagrees. As stated above in section 10-3, the location of a user requesting data (from a 2nd location) is compared to that of where the data is presently location (a 1st location). Paragraph 0099 further discloses that in the authentication process for the request for transmission of the data to the 2nd location, the location of user device 104 is verified and is authenticated "employing techniques described" within the disclosure of Roese, such as those described in section 10-2A and 10-2C, such as the example given in that of the "campus" boundary. Using the "campus" boundary example with Fig. 8, the first and second devices that are "verified and authenticated" are in a common "domain", or within a group of networked computers, as is seen in Fig. 8. Appellant's specification supplies no definition for "common domain", and thus the limitation will be interpreted with the common definitions of the claim language used.

5. Rejection of claim 9 under 35 U.S.C. 102 using Roese

Regarding Appellant's argument alleging the paragraphs and figures cited by the Examiner (Para. 100-103 and Figs. 1 and 8) do not disclose "network devices associated with a single family", the Examiner respectfully disagrees. As stated above in section 10-3, the paragraphs of 100-103 are more detailed explanation as to features explained in Paragraphs 0096-0099, wherein the location of a user requesting data

(from a 2nd location) is compared to that of where the data is presently location (a 1st location). As seen above in section 10-4, computer devices that are established as verified and authenticated by employing techniques, such as the "campus" boundary state by which locations are compared as seen in section 10-2A and 10-2C, the computer devices (devices at first and second addresses) are interpreted do be associated with a common domain, or family, or group of networked computers. The Examiner refers to section 10-2D regarding the lack of further definition for claim limitation "family".

6. Rejection of claim 11 under 35 U.S.C. 102 using Roese

A. Regarding Appellant's argument alleging "Roese does not include additional data in his packet that can have two states, respectively indicating the two claimed restrictions on re-transmission" (Page 16, Para. 2), the Examiner respectfully disagrees. The Examiner disclosed Roese's disclosure of these claim limitations in section 10-2A.

B. Regarding Appellant's argument alleging "Roese does not teach an arrangement in which a decision whether to re-transmit a content packet to a second destination address…is a function of the first destination address" (Page 16, Para. 3), the Examiner respectfully disagrees. The Examiner disclosed Roese's disclosure of these claim limitations in section 10-2E.

7. Rejection of claim 13 under 35 U.S.C. 102 using Roese

Regarding Appellant's argument alleging "a campus is not a 'single family' as

claimed" (Page 16, Para. 7), the Examiner respectfully disagrees. The Examiner

disclosed Appellant's lack of supported reasoning and further definition of the claim

limitation in the specification in section 10-2D.

8. Rejection of claim 14 under 35 U.S.C. 102 using Roese

Regarding Appellant's argument alleging the paragraphs cited by the Examiner in

the Office Action dated 04/21/2009 "do not concern re-distribution of entertainment

content from an intended destination address to a second address" (Page 13, Para 2),

the Examiner respectfully disagrees. The Examiner disclosed Roese's disclosure of

these claim limitations in section 10-3.

9. Rejection of claim 15 under 35 U.S.C. 102 using Roese

Regarding Appellant's argument alleging the figures cited by the Examiner (Figs.

1 and 8) "have no teachings about a common domain", the Examiner respectfully

disagrees. The Examiner disclosed Roese's disclosure of these claim limitations in

section 10-4.

10. Rejection of claim 16 under 35 U.S.C. 102 using Roese

Regarding Appellant's argument alleging the paragraphs and figures cited by the

Examiner (Para. 100-103 and Figs. 1 and 8) do not disclose "network devices

associated with a single family", the Examiner respectfully disagrees. The Examiner

disclosed Roese's disclosure of these claim limitations in section 10-5.

11. Rejection of claim 17 under 35 U.S.C. 102 using Roese

In response to applicant's argument that the references fail to show certain

features of applicant's invention, it is noted that the features upon which applicant relies

(i.e., "Roese does not teach the use of a firewall to determine whether device are

physically remote or not") are not recited in the rejected claim(s). Although the claims

are interpreted in light of the specification, limitations from the specification are not read

into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir.

1993).

12. Rejection of claim 1 under 35 U.S.C. 103 using Roese in view of Levy '899

A. Regarding Appellant's argument alleging Roese "does not teach use of a

firewall to define the geography of the boundary" (Page 19, Para. 3), the Examiner

respectfully disagrees. The claim limitation reads "defining a geographical boundary

across which certain content data does not pass, wherein said boundary is defined – **at**

least in part – by a hardware firewall device;" (emphasis added). The broad claim

language of "at least in part" causes what the role that the hardware firewall plays in the

step of the method to be indefinite or ambiguous. As seen in the Office Action dated

04/21/2009, Roese discloses firewalls "to analyze packets and, from that analysis, make

a determination as to whether packet transmission into or out of the network is

permitted", which is interpreted to meet the part of the method step including the limitation of certain "content data does not pass".

B. Regarding Appellant's argument alleging Roese does not disclose "any teaching of single-bit flags" (while referencing the Examiner's rejection of claims 29-31 wherein the statement of "Roese…do not explicitly state the use of a single bit flag") (Page 20, Para. 1), the Examiner respectfully disagrees. Comparing claims 29-31 to claim 1 will show that claims 29-31 explicitly recite "one single-bit flag" or "a single-bit flag", whereas claim 1 explicitly recites "one or more single-bit flags". These limitations are fundamentally different in that the limitation of claim 1 is broader than that of claims 29-31. Header data of an IP packet necessarily must necessarily contain "one or more bits" in a digital system to represent restriction information/data (i.e. it cannot be represented by zero bits). Furthermore, the flags are interpreted as indications, as in indications as to the location. The Examiner relied on the broadest reasonable interpretation of the limitation of "flags" in order to be consistent with the brevity of the claim terminology found in the specification in a manner that would be supported under 35 U.S.C. 112 1st. Appellant's specification merely possesses a passing reference to the use of flags (Page 3, Lines 7-9).

C. Regarding Appellant's argument alleging Roese "does not teach or suggest watermarking", the Examiner respectfully points out that Roese is not relied upon to teach watermarking. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642

F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231

USPQ 375 (Fed. Cir. 1986).

     D. Regarding Appellant's argument alleging "an artisan would not employ

watermarking to provide 'restriction information hidden from a user'... if the restriction

information is also exposed in the packet header" (Page 22, Para. 3), the Examiner

respectfully disagrees. As set forth in the rejection, Roese teaches the modification of

packets with additional data based on tags, such that the additional data may conveys

restriction information on the data in the packets for devices to determine whether to

prohibit or allow transmission of packets, and Levy '899 teaches preserving watermarks

of digital content during transmission in a packet-based communication channel via

transmarking an initial digital watermark of the content into watermark payloads in each

packet with additional data placed in each packet header based on the watermark

payload. The known technique of Levy '899 is applied to the known method of Roese to

predictably improve the method in the manner of in the event of replacing a packet

header that previously possesses a watermark reference, the substitution of a header

without that watermark reference would result in a situation wherein the header no

longer references the watermark in the payload, thus making the watermarked

information in the payload corrupt, or unreadable. A simple combination of elements,

irrespective of whether it is duplicative, does not render it unobvious.

     <u>13. Rejection of claims 10 and 18 under 35 U.S.C. 103 using Roese in view of</u>

<u>Levy '899</u>

Regarding Appellant's argument alleging failed establishment of *prima facie*

obviousness (Page 23, Para. 1), the Examiner addressed these arguments in section

10-12.

14. Rejection of claim 25 under 35 U.S.C. 103 using Roese in view of Levy '899

A. Regarding Appellant's argument alleging Roese "does not disclose a

computing device in a consumer's home network that divides video entertainment

among payload portions of plural IP packets" because "in Roese, the dividing of content

into packet form is understood to be done by a remote party. No device at a consumer's

home performs this act" (Page 24, Para. 3), the Examiner respectfully disagrees. Any IP

traffic sent from the client (or "home") devices of Roese will necessarily divide the

information into multiple IP packets in order to be transported in conjunction with the

TCP/IP standard.

B. Regarding Appellant's argument alleging Roese "does not teach a home

networking device that refuses to transmit packets 'to a different network if the included

data indicates that the video entertainment should not be redistributed from the

consumer's home network. No device at consumer's home performs this act" (Page 24,

Para. 4), the Examiner respectfully disagrees. Roese discloses a networking device in

that of the firewall, which performs the refusing step as stated in the Office Action dated

04/21/2009 for a domain, seen in Fig. 8. The domain, as previously established can be

that of a room, building (or house), or campus, all of which are interpreted as home

locations (interpreted as relating to any location where one can live, reside, or dwell).

C. Regarding Appellant's argument alleging failed establishment of *prima facie*
obviousness (Page 25 Para. 1), the Examiner addressed these arguments in section
10-12.

15. Rejection of claim 26 under 35 U.S.C. 103 using Roese in view of Levy '899

Regarding Appellant's argument alleging Levy does not disclose "the
'ascertaining…' of restriction information must precede 'including…' data related to the
restriction in header portions of each of the IP packets" (Page 25, Para. 5), the
Examiner respectfully disagrees. In response to applicant's arguments against the
references individually, one cannot show nonobviousness by attacking references
individually where the rejections are based on combinations of references. See *In re
Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091,
231 USPQ 375 (Fed. Cir. 1986).

16. Rejection of claim 28 under 35 U.S.C. 103 using Roese in view of Levy '899

Regarding Appellant's argument alleging Levy does not disclose "the
'ascertaining…' of restriction information must precede 'including…' data related to the
restriction in header portions of each of the IP packets" (Page 26, Para. 2), the
Examiner respectfully disagrees. In response to applicant's arguments against the
references individually, one cannot show nonobviousness by attacking references
individually where the rejections are based on combinations of references. See *In re*

Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091,

231 USPQ 375 (Fed. Cir. 1986).

      17. Rejection of claim 27 under 35 U.S.C. 103 using Roese in view of Levy '899,
and further in view of Levy '844

      Regarding Appellant's argument alleging failed establishment of *prima facie*

obviousness (Page 27, Para. 1), the Examiner addressed these arguments in section

10-12.

      18. Rejection of claims 29-31 under 35 U.S.C. 103 using Roese in view of Levy
'899, and further in view of Medvinsky

      Regarding Appellant's arguments regarding the allowability of claims 29-31 due

to their "standing or falling" with claims 1, 4, and 11, the Examiner has shown the

rejection of claims 1, 4, and 11 to be valid and the claims to not be allowable. Therefore,

claims 29-31 would remain rejected.

(11) Related Proceeding(s) Appendix

      No decision rendered by a court or the Board is identified by the examiner in the

Related Appeals and Interferences section of this examiner's answer.

      For the above reasons, it is believed that the rejections should be sustained.

      Respectfully submitted,

      /Nicholas Corbo/

Patent Examiner, Art Unit 2427

02/22/2010

Conferees:

/Scott Beliveau/

Supervisory Patent Examiner, Art Unit 2427

/Jason P Salce/

Primary Examiner, Art Unit 2421